AS

(19) JAPANESE PATENT OFFICE

PATENT ABSTRACTS OF JAPAN

(11) Publication number: 2000165376 A

(43) Date of publication of application: 16.06.00

(51) Int. Cl H04L 9/14
G11B 20/10
H04L 9/32
H04L 12/28

(21) Application number: 10333216

(22) Date of filing: 24.11.98

(71) Applicant: MATSUSHITA ELECTRIC IND CO LTD

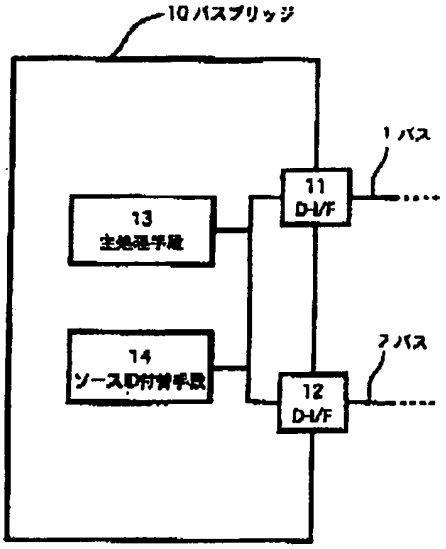
(72) Inventor: YAMADA MASAZUMI
IIZUKA HIROYUKI
NISHIMURA TAKUYA
TAKECHI HIDEAKI
KUNO YOSHIKI
HAMAMOTO YASUO

(54) BUS BRIDGE AND RECORDING MEDIUM

(57) Abstract:

PROBLEM TO BE SOLVED: To provide a bus bridge by which a device at a destination can discriminate a sender device directly or indirectly in the case of conducting data transfer using a data packet like an isochronous packet among different buses in compliance with the AV protocol where the sender device can be specified only in a single bus.

SOLUTION. The bus bridge 10 consists of D-I/F 11, 12 that transfer data directly to buses 1, 2, a main processing means 13 that applies processing such as clock adjustment processing similar to that for a conventional bus bridge to a packet sent from each bus and a source ID replacement means 14. The source ID replacement means 14 uses a source ID in an isochronous packet for a node ID to specify the bus bridge 10 in a destination bus or replaces a node to specify the sender device in a sender bus with a node ID to specify the bus bridge in a destination bus.



(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－165376
（P2000－165376A）
(43)公開日　平成12年６月16日(2000.6.16)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード（参考）
Ｈ０４Ｌ　9/14		Ｈ０４Ｌ　9/00	６４１	５Ｄ０４４
Ｇ１１Ｂ　20/10		Ｇ１１Ｂ　20/10	Ｄ	５Ｊ１０４
Ｈ０４Ｌ　9/32		Ｈ０４Ｌ　9/00	６７５Ａ	５Ｋ０３３
12/28		11/00	３１０Ｚ	

審査請求　未請求　請求項の数15　ＯＬ　（全 17 頁）

(21)出願番号　特願平10－333216

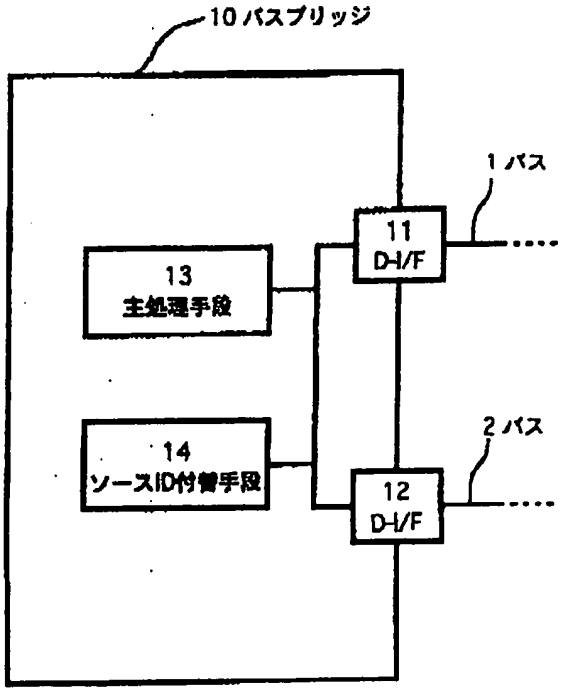
(22)出願日　平成10年11月24日(1998.11.24)

(71)出願人　000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地
(72)発明者　山田　正純
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(72)発明者　堀塚　裕之
大阪府門真市大字門真1006番地　松下電器産業株式会社内
(74)代理人　100092794
弁理士　松田　正道

最終頁に続く

(54)【発明の名称】　バスブリッジおよび記録媒体

(57)【要約】
【課題】　ＡＶプロトコルに準拠したアイソクロノスパケットのような単一バス内でのみ送信元の機器を特定できるようなデータパケットによるデータ転送を、異なるバス間にまたがって行う場合において、受信先の機器が直接または間接的に送信元の機器を判別できるバスブリッジを提供する。
【解決手段】　バスブリッジ１０は、バス１、２と直接データの転送を行うＤ－Ｉ／Ｆ１１、１２と、各バスから送信されてきたパケットに対してクロック調整処理等の従来のバスブリッジと同様の処理を行う主処理手段１３と、ソースＩＤ付替手段１４とで構成されており、ソースＩＤ付替手段１４は、アイソクロノスパケットのソースＩＤを、受信先バス内でバスブリッジ１０を特定するノードＩＤとする、または、送信元バス内で送信元機器を特定するノードＩＤから、受信先バス内でバスブリッジ１０を特定するノードＩＤに付け替える。



1

【特許請求の範囲】

【請求項１】 それぞれに一つまたは複数の機器が接続された複数のバス間を接続し、異なる前記バスにそれぞれ接続されている前記機器間のデータ転送を仲介するバスブリッジにおいて、

前記データ転送を仲介されるストリームの送信元機器が接続されている前記バスを送信元バスとし、前記ストリームの受信先機器が接続されている前記バスを受信先バスとすると、

前記ストリームのデータ用パケットの送信元の識別子であるソースＩＤを、前記受信先バス内で前記バスブリッジ自身を特定するノードＩＤとする、または、前記送信元バス内で前記送信元機器を特定するノードＩＤから、前記受信先バス内で前記バスブリッジ自身を特定するノードＩＤに付け替えるＩＤ付替手段を備えることを特徴とするバスブリッジ。

【請求項２】 前記ストリームのデータが、暗号化鍵により暗号化されて送信される場合、

前記受信先機器からの前記ストリームに対応する認証要求および認証の手続きに関するパケットを前記送信元機器へ送信する認証要求送受信手段と、

前記送信元機器から前記ストリームに対応する前記暗号化鍵および認証の手続きに関するパケットを受信して前記受信先機器へ送信する暗号化鍵送受信手段と、

前記送信元機器から、前記ストリームに対応し、前記暗号化鍵によって暗号化された前記データを受信して前記受信先機器へ送信するデータ送受信手段と、

前記認証要求および認証の手続きに関するパケットを前記送信元機器へ送信する際、前記認証要求および認証の手続きに関するパケットの受信先の識別子であるディスティネーションＩＤを、前記受信先バスを特定するバスＩＤと前記受信先バス内で前記バスブリッジ自身を特定するノードＩＤとの組合せから、前記送信元バスを特定するバスＩＤと前記送信元バス内で前記送信元機器を特定するノードＩＤとの組合せに付け替え、前記認証要求および認証の手続きに関するパケットの送信元の識別子であるソースＩＤを、前記受信先バスを特定するバスＩＤと前記受信先バス内で前記受信先機器を特定するノードＩＤとの組合せから、前記送信元バスを特定するバスＩＤと前記送信元バス内で前記バスブリッジ自身を特定するノードＩＤとの組合せに付け替え、前記暗号化鍵および認証の手続きに関するパケットを前記受信先機器へ送信する際、前記暗号化鍵および認証の手続きに関するパケットの受信先の識別子であるディスティネーションＩＤを、前記送信元バスを特定するバスＩＤと前記送信元バス内で前記バスブリッジ自身を特定するノードＩＤとの組合せから、前記受信先バスを特定するバスＩＤと前記受信先バス内で前記受信先機器を特定するノードＩＤとの組合せに付け替え、前記暗号化鍵および認証の手続きに関するパケットの送信元の識別子であるソースＩＤを、前記送信元バスを特定するバスＩＤと前記送信元バス内で前記送信元機器を特定するノードＩＤとの組合せから、前記受信先バスを特定するバスＩＤと前記受信先バス内で前記バスブリッジ自身を特定するノードＩＤとの組合せに付け替える第２のＩＤ付替手段とを備えることを特徴とする請求項１に記載のバスブリッジ。

【請求項３】 前記受信先バス内で前記バスブリッジ自身を特定する前記ノードＩＤ１つに対して、前記受信先バスに前記受信先バス以外の前記バスから転送される前記ストリーム数を、使用許諾情報のうちデータ暗号化を要する種類毎に１つ以下に制限することを特徴とする請求項２に記載のバスブリッジ。

【請求項４】 前記ストリームのデータが、暗号化鍵により暗号化されて送信される場合、

前記受信先機器からの前記ストリームに対応する認証要求および認証の手続きに関するパケットを前記送信元機器へ送信する認証要求送受信手段と、

前記送信元機器から前記ストリームに対応する前記暗号化鍵および認証の手続きに関するパケットを受信して前記受信先機器へ送信する暗号化鍵送受信手段と、

前記送信元機器から、前記ストリームに対応し、前記暗号化鍵によって暗号化された前記データを受信して前記受信先機器へ送信するデータ送受信手段と、

前記送信元バスおよび前記送信元機器を特定できる送信元識別子を、前記データ用パケットの所定の位置に書き込む識別子書込手段とを備え、

前記受信先機器は、前記データ用パケットから前記送信元識別子を読み取り、前記認証要求および認証の手続きに関するパケットの所定の位置に、前記受信先バスおよび前記受信先機器自身を特定できる受信先識別子および前記送信元識別子を書き込んで送信し、

前記認証要求送受信手段は、前記認証要求および認証の手続きに関するパケットを受信して、前記送信元識別子を読み取り、これに基づいて、前記認証要求および認証の手続きに関するパケットを前記送信元機器へ送信し、

前記送信元機器は、前記認証要求および認証の手続きに関するパケットを受信して、前記送信元識別子を読み取り、前記暗号化鍵および認証の手続きに関するパケットの所定の位置に、前記送信元識別子および前記受信先識別子を書き込んで送信し、

前記暗号化鍵送受信手段は、前記暗号化鍵および認証の手続きに関するパケットを受信して、前記受信先識別子を読み取り、これに基づいて、前記暗号化鍵および認証の手続きに関するパケットを前記受信先機器へ送信することを特徴とする請求項１に記載のバスブリッジ。

【請求項５】 前記受信先機器は、前記認証要求および認証の手続きに関するパケットの前記ソースＩＤおよび前記ディスティネーションＩＤの位置に、それぞれ前記受信先識別子および前記送信元識別子を書き込んで送信し、

前記送信元機器は、前記暗号化鍵および認証の手続きに関するパケットの前記ソースＩＤおよび前記ディスティネーションＩＤの位置に、それぞれ前記送信元識別子および前記受信先識別子を書き込んで送信することを特徴とする請求項４に記載のバスブリッジ。

【請求項６】　前記ストリームのデータが、暗号化鍵により暗号化されて送信される場合、

前記送信元機器および前記受信先機器とそれぞれ前記ストリームに対応する認証を行う認証手段と、

前記送信元機器から受け渡された、前記ストリームに対応する前記暗号化鍵を保持し、これを、前記受信先機器からの要求に応じて、前記受信先機器へ送信する暗号化鍵保持手段とを備えることを特徴とする請求項１に記載のバスブリッジ。

【請求項７】　前記受信先バス内で前記バスブリッジ自身を特定する前記ノードＩＤ１つに対して、前記受信先バスに前記受信先バス以外の前記バスから転送される前記ストリーム数を、使用許諾情報のうちデータ暗号化を要する種類毎に１つ以下に制限することを特徴とする請求項６に記載のバスブリッジ。

【請求項８】　前記暗号化鍵は、定期的または不定期的に更新生成されるデータ暗号化鍵と、前記データ暗号化鍵の暗号化に用いる鍵交換用鍵とで構成され、

前記データ暗号化鍵は、送信時においては、前記鍵交換用鍵により暗号化されていることを特徴とする請求項２～７のいずれかに記載のバスブリッジ。

【請求項９】　前記ストリームのデータが、暗号化鍵により暗号化されて送信される場合、

前記送信元機器および前記受信先機器とそれぞれ前記ストリームに対応する認証を行う認証手段と、

前記データを前記暗号化鍵によって解読する暗号解読手段と、

前記解読されたデータをブリッジ用鍵によって再暗号化する再暗号化手段と、

前記送信元機器から、前記ストリームに対応する前記暗号化鍵、および、前記暗号化鍵によって暗号化された前記ストリームに対応する前記データを受信する受信手段と、

前記ブリッジ用鍵と前記再暗号化されたデータとを前記受信先機器へ送信する送信手段とを備えることを特徴とする請求項１に記載のバスブリッジ。

【請求項１０】　前記ブリッジ用鍵は、１つの前記ストリームに対応する前記暗号化鍵と同じものであり、

前記ブリッジ用鍵と同じ前記暗号化鍵により暗号化された前記データは、前記暗号解読手段による解読および前記再暗号化手段による再暗号化を行われずに、前記受信先機器へ送信されることを特徴とする請求項９に記載のバスブリッジ。

【請求項１１】　前記暗号化鍵は、定期的または不定期的に更新生成されるデータ暗号化鍵と、前記データ暗号

化鍵の暗号化に用いる鍵交換用鍵とで構成され、

前記データ暗号化鍵は、送信時においては、前記鍵交換用鍵により暗号化されており、

前記ブリッジ用鍵は、定期的または不定期的に更新生成されるブリッジ用暗号化鍵と、前記ブリッジ用暗号化鍵の暗号化に用いるブリッジ用鍵交換用鍵とで構成され、

前記受信手段は、前記送信元機器から、前記データ暗号化鍵によって暗号化された前記データ、前記鍵交換用鍵によって暗号化された前記データ暗号化鍵および前記鍵交換用鍵を受信し、

前記暗号解読手段は、前記データ暗号化鍵を前記鍵交換用鍵によって解読し、前記データを前記解読されたデータ暗号化鍵によって解読し、

前記再暗号化手段は、前記解読されたデータを前記ブリッジ用暗号化鍵によって再暗号化し、前記ブリッジ用暗号化鍵を前記ブリッジ用鍵交換用鍵によって再暗号化し、

前記送信手段は、前記ブリッジ用鍵交換用鍵、前記ブリッジ用鍵交換用鍵によって再暗号化された前記ブリッジ用暗号化鍵と、前記ブリッジ用暗号化鍵によって再暗号化された前記データとを前記受信先機器へ送信することを特徴とする請求項９に記載のバスブリッジ。

【請求項１２】　前記ブリッジ用暗号化鍵および前記ブリッジ用鍵交換用鍵は、１つの前記ストリームに対応する前記データ暗号化鍵および前記鍵交換用鍵とそれぞれ同じものであり、

前記１つのストリームに対応する前記データ、前記データ暗号化鍵および前記鍵交換用鍵の転送を行う場合、

前記ブリッジ用暗号化鍵と同じ前記データ暗号化鍵により暗号化された前記データおよび前記ブリッジ用鍵交換用鍵と同じ前記鍵交換用鍵により暗号化された前記データ暗号化鍵は、前記暗号解読手段による解読および前記再暗号化手段による再暗号化を行われずに、前記受信先機器へ送信されることを特徴とする請求項１１に記載のバスブリッジ。

【請求項１３】　前記ブリッジ用暗号化鍵は、１つの前記ストリームに対応する前記データ暗号化鍵と同じものであり、

前記１つのストリームに対応する前記データ、前記データ暗号化鍵および前記鍵交換用鍵の転送を行う場合、

前記受信手段は、前記送信元機器から、前記データ暗号化鍵によって暗号化された前記データ、前記鍵交換用鍵によって暗号化された前記データ暗号化鍵および前記鍵交換用鍵を受信し、

前記暗号解読手段は、前記データ暗号化鍵を前記鍵交換用鍵によって解読し、

前記再暗号化手段は、前記データ暗号化鍵を前記ブリッジ用暗号化鍵とし、これを前記ブリッジ用鍵交換用鍵によって再暗号化し、

前記送信手段は、前記ブリッジ用鍵交換用鍵、前記ブリ

ッジ用鍵交換用鍵によって再暗号化された前記ブリッジ用暗号化鍵と、前記暗号解読手段による解読および前記再暗号化手段による再暗号化が行われなかった前記データとを前記受信先機器へ送信することを特徴とする請求項１１に記載のバスブリッジ。

【請求項１４】　前記ブリッジ用鍵交換用鍵は、１つの前記ストリームに対応する前記鍵交換用鍵と同じものであり、

前記１つのストリームに対応する前記データ、前記データ暗号化鍵および前記鍵交換鍵の転送を行う場合、

前記受信手段は、前記送信元機器から、前記データ暗号化鍵によって暗号化された前記データ、前記鍵交換用鍵によって暗号化された前記データ暗号化鍵および前記鍵交換用鍵を受信し、

前記暗号解読手段は、前記データ暗号化鍵を前記鍵交換用鍵によって解読し、前記データを前記解読されたデータ暗号化鍵によって解読し、

前記再暗号化手段は、前記解読されたデータを前記ブリッジ用暗号化鍵によって再暗号化し、前記鍵交換用鍵を前記ブリッジ用鍵交換用鍵とし、これによって前記ブリッジ用暗号化鍵を再暗号化し、

前記送信手段は、前記ブリッジ用鍵交換用鍵、前記ブリッジ用鍵交換用鍵によって再暗号化された前記ブリッジ用暗号化鍵と、前記ブリッジ用暗号化鍵によって再暗号化された前記データとを前記受信先機器へ送信することを特徴とする請求項１１に記載のバスブリッジ。

【請求項１５】　請求項１～１４のいずれかに記載の、各手段の機能の全部または一部をコンピュータに実行させるプログラムを格納することを特徴とする記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、それぞれに一つまたは複数の機器が接続された複数のバス間を接続し、異なる前記バスにそれぞれ接続されている前記機器間のデータ転送を仲介するバスブリッジ、および、前記バスブリッジの各手段の機能の全部または一部をコンピュータに実行させるプログラムを格納する記録媒体に関するものである。

【０００２】

【従来の技術】大量のデータ転送を高速かつ高品質に行えるディジタル・インターフェースとし、ＩＥＥＥ１３９４規格（IEEE:THE INSTITUTE OF ELECTRICAL AND ELECTRINIC ENGINEERS, INC）を用いた高速シリアル・バス・インターフェース（以下、「ＩＥＥＥ１３９４バス」と記す。）が近年注目されてきている。

【０００３】ＩＥＥＥ１３９４規格におけるデータ転送には、映像信号や音声信号等の同期データの転送に適したアイソクロノス通信と、制御信号等の非同期データの転送に適したエイシンクロナス通信とがあり、両通信はＩＥＥＥ１３９４バス上で混在することが可能である。

【０００４】アイソクロノス通信は、いわゆる放送型の通信であり、ＩＥＥＥ１３９４バス上のある装置が出力するアイソクロノスパケットは、同バス上の全ての装置が受信することができる。

【０００５】これに対してエイシンクロナス通信は、１対１の通信と放送型通信の両方がある。そして、バス上のある装置が出力するエイシンクロナスパケットには、パケットヘッダー内に、そのパケットを受信すべき装置をあらわす識別子であるディスティネーションＩＤが含まれており、そのディスティネーションＩＤが特定の装置をあらわす時にはその識別子で指定された装置が当該エイシンクロナスパケットを受信し、ディスティネーションＩＤがブロードキャストをあらわす時には同バス上の全ての装置が当該エイシンクロナスパケットを受信する。なお、エイシンクロナスパケットには、パケットヘッダー内に、そのパケットを送信している送信装置をあらわす識別子であるソースＩＤも含まれている。このディスティネーションＩＤおよびソースＩＤには、それぞれ１６ビットが割り当てられており、そのうちの１０ビットには機器が接続されているバスを特定するバスＩＤが書き込まれ、６ビットにはバス内で当該機器を特定するノードＩＤが書き込まれる。

【０００６】また、ＩＥＥＥ１３９４規格を用いてディジタル音声信号やディジタル映像信号等を転送したり、ＩＥＥＥ１３９４バス上につながれた機器間でデータ伝送経路の接続管理を行うための規格として、ＩＥＣ（IEC：International Electronical Commission 国際電気標準会議）においてＩＥＣ６１８８３規格（以下、「ＡＶプロトコル」と記す。）が検討されている。ＡＶプロトコルにおいては、映像音声データはアイソクロノスパケット内に配置されて転送される。また、アイソクロノスパケットはＣＩＰヘッダ（CIP：Common Isochronous Packet）を含む。ＣＩＰヘッダ内には映像音声データの種類を示す識別情報や、アイソクロノスパケットを送信している送信装置の装置をあらわす識別子であるソースＩＤ等の情報が含まれている。

【０００７】図５は、ＡＶプロトコルに準拠したアイソクロノスパケットのフォーマットを示す図である。アイソクロノスパケットは、アイソクロノスパケットヘッダ９００、ヘッダＣＲＣ９０１、アイソクロノスペイロード９０２、データＣＲＣ９０３からなる。

【０００８】アイソクロノスパケットヘッダ９００にはタグ９０７が含まれる。タグ９０７は、その値が１である時には、そのアイソクロノスパケットがＡＶプロトコルに準拠したアイソクロノスパケットであることを示す。タグ９０７の値が１であるとき、即ち、そのアイソクロノスパケットがＡＶプロトコル準拠のアイソクロノスパケットである時には、アイソクロノスペイロード９０２の先頭にＣＩＰヘッダ９０４が含まれる。

【０００９】また、アイソクロノスパケットヘッダ９０

０中のＣｈａｎｎｅｌフィールド９１１には、バス内での転送に用いられているチャンネル番号が書き込まれる。

【００１０】また、アイソクロノスパケットヘッダ９００には、Ｓｙフィールド９１０が含まれる。ＡＶプロトコル準拠のアイソクロノスパケットである時には、Ｓｙフィールドはデータ保護情報（使用許諾情報）等を格納するために使用される。具体的にはＥＭＩ（Ｅｎｃｒｙｐｔｉｏｎ Ｍｏｄｅ Ｉｎｄｉｃａｔｏｒ）と呼ばれる使用許諾情報の代表値およびデータ暗号化モードを示す２ビットの情報と、データ暗号化鍵の更新タイミングを示すＯｄｄ／Ｅｖｅｎフラグと呼ばれる１ビットの情報を含む。Ｓｙフィールド９１０に格納されたＥＭＩ値が「００」である時には、送信対象となるデータ（後述する実データ９０５）が、コピーが自由に行えるデータである事を示している。また、「１０」である時には、そのデータが、１回のみコピー可能であることを、更に、「１１」である時には、そのデータが、コピー禁止であることを示している。

【００１１】ＣＩＰヘッダ９０４の中には、当該アイソクロノスパケットを出力している送信元の装置の識別子であるソースＩＤ９０６が含まれる。このソースＩＤ９０６は、６ビットの長さを有しており、一つのバス内で当該発信元の機器を特定するノードＩＤが書き込まれる。

【００１２】また、ＣＩＰヘッダ９０４には、アイソクロノスペイロード９０２に含まれる実データ９０５がどの様な種類のデータであるかをあらわすＦＭＴ９０８やＦＤＦ９０９が含まれる。

【００１３】映像や音声の送信対象となるデータは実データ９０５に含まれるが、この実データ９０５は、上述したＥＭＩ値が、「１０」または「１１」である場合には、暗号化されたデータであるが、コピーフリーを意味する「００」の場合には、暗号化はされていない。また、実際の使用許諾情報は、実データ９０５中に含まれており、一般に、ＣＤの場合はＳＣＭＳと、また、ＤＶの場合はＣＧＭＳ等と呼ばれている。

【００１４】以上のようなＩＥＥＥ１３９４バスを複数個接続して、異なるＩＥＥＥ１３９４バスにそれぞれ接続されている機器間のデータ転送を仲介するバスブリッジが提案されている。図６は、バスブリッジによってデータ転送の仲介が行われる２つのＩＥＥＥ１３９４バスを示す概略構成図である。バス１には複数の機器１０１、１０２、１０３、・・・が接続されており、バス２には複数の機器２０１、２０２、２０３、・・・が接続されている。バスブリッジ１００は、バス１、２に接続されており、それぞれのバスに接続されている前記機器間のデータ転送を仲介するものである。

【００１５】図６のバスブリッジ１００のようにＩＥＥＥ１３９４バスが接続されたバスブリッジの機能として

は、異なるバスブリッジに接続された機器間のデータ転送において、バス間のクロックの調整を行うこと、送信元のバス側のアイソクロノス・リソースのコピー（帯域確保）、すなわち、バス１中でアイソクロノス通信用に確保された帯域用のパラメータをバス２側でも同様に確保することを行うこと等が挙げられる。

【００１６】

【発明が解決しようとする課題】しかしながら、図６で示したようなバスブリッジにおいて、図５で示したようなＡＶプロトコルに準拠したアイソクロノスパケットによって、データ転送を行う場合、アイソクロノスパケット中のソースＩＤ９０６には、バス毎に送信元の機器を特定するノードＩＤが書き込まれるだけで、異なるバス間にまたがったデータ転送を行う場合においては、当該パケットが、受信側と同一のバスに接続された機器から送信されたパケットなのか、異なるバスに接続された機器から送信されたパケットなのか、判別がつかなくなってしまう。

【００１７】すなわち、図６において、アイソクロノスパケットがバス１に接続された機器１０３から出力されたものであるとすると、当該アイソクロノスパケット中のソースＩＤ９０６には、バス１内で機器１０３を特定するための識別子であるノードＩＤ「３」が書き込まれている。このアイソクロノスパケットがバスブリッジ１００を介してバス２側へ転送され、バス２に接続された機器２０２が受信したとすると、機器２０２は、当該アイソクロノスパケットが、機器１０３から送信されてきたものなのか、機器２０３から送信されてきたものなのか、判別がつかなくなってしまう。

【００１８】ソースＩＤ９０６にノードＩＤだけでなく、バスを特定するバスＩＤ（１０ビット）を書き込めれば、上記問題は解決するが、ノードＩＤは６ビットで定義されるものであり、アイソクロノスパケット中のソースＩＤ９０６は６ビットの割り当てしかないため、バスＩＤの書込が行われる余地はない。

【００１９】通常のアイソクロノスパケットによるデータ転送は、放送型の１方向転送であるため、上述したような送信元の機器を判別する必要はないが、転送されるデータの内容・特性等によっては、送信元の機器を判別する必要が生じる。特に、アイソクロノスパケット中のＳｙフィールド９１０に格納されたＥＭＩ値が「１０」または「１１」である場合、すなわち、当該アイソクロノスパケットのデータが、１回のみコピー可能である、または、コピー禁止である場合には、実データは暗号化が施されて転送されるため、暗号解読用の鍵の受け渡しのための認証等を送信元の機器と行う必要があるため、送信元の機器の判別は不可欠なものとなってくる。また、ＩＥＥＥ１３９４バスにおいては、同一機器から送信される暗号化データの暗号化鍵は前記ＥＭＩ値の示す暗号化モード毎、すなわちデータ暗号化を要する種類毎

に同一のものを用いることにしているため、受信先バスであるバス２内では、同一のノードＩＤ、同一種類のＥＭＩに対して、２つ以上の異なった暗号化鍵が使われているようにみなされてしまい、受信側の機器２０２では、どの暗号化鍵によってデータ解読を行うのかが判別できなくなってしまう。さらに、送信元の機器が暗号化鍵を定期的または不定期的に更新する場合においては、機器毎に更新のタイミングが異なるので、解読に真に必要な鍵を受信側機器が判別することは困難である。

【００２０】本発明は、上述した従来のバスブリッジが有する課題を考慮し、ＡＶプロトコルに準拠したアイソクロノスパケットのような単一バス内でのみ送信元の機器を特定できるようなデータパケットによるデータ転送を、異なるバス間にまたがって行う場合において、受信先の機器が直接または間接的に送信元の機器を判別できるバスブリッジを提供することを目的とするものである。さらに、上記に加えて、実データが暗号化されて送信される場合、前記送信元の機器と前記受信先の機器との間での認証・鍵交換が確実に行われるバスブリッジを提供することを目的とするものである。

【００２１】また、前記バスブリッジの各手段の機能の全部または一部をコンピュータに実行させるプログラムを格納する記録媒体を提供することを目的とするものである。

【００２２】

【課題を解決するための手段】上述した課題を解決するために、第１の本発明（請求項１に記載の本発明に対応）は、それぞれに一つまたは複数の機器が接続された複数のバス間を接続し、異なる前記バスにそれぞれ接続されている前記機器間のデータ転送を仲介するバスブリッジにおいて、前記データ転送を仲介されるストリームの送信元機器が接続されている前記バスを送信元バスとし、前記ストリームの受信先機器が接続されている前記バスを受信先バスとすると、前記ストリームのデータ用パケットの送信元の識別子であるソースＩＤを、前記受信先バス内で前記バスブリッジ自身を特定するノードＩＤとする、または、前記送信元バス内で前記送信元機器を特定するノードＩＤから、前記受信先バス内で前記バスブリッジ自身を特定するノードＩＤに付け替えるＩＤ付替手段を備えることを特徴とするバスブリッジである。

【００２３】また、第２の本発明（請求項２に記載の本発明に対応）は、前記ストリームのデータが、暗号化鍵により暗号化されて送信される場合、前記受信先機器からの前記ストリームに対応する認証要求および認証の手続きに関するパケットを前記送信元機器へ送信する認証要求送受信手段と、前記送信元機器から前記ストリームに対応する前記暗号化鍵および認証の手続きに関するパケットを受信して前記受信先機器へ送信する暗号化鍵送受信手段と、前記送信元機器から、前記ストリームに対応し、前記暗号化鍵によって暗号化された前記データを受信して前記受信先機器へ送信するデータ送受信手段と、前記認証要求および認証の手続きに関するパケットを前記送信元機器へ送信する際、前記認証要求および認証の手続きに関するパケットの受信先の識別子であるディスティネーションＩＤを、前記受信先バスを特定するバスＩＤと前記受信先バス内で前記バスブリッジ自身を特定するノードＩＤとの組合せから、前記送信元バスを特定するバスＩＤと前記送信元バス内で前記送信元機器を特定するノードＩＤとの組合せに付け替え、前記認証要求および認証の手続きに関するパケットの送信元の識別子であるソースＩＤを、前記受信先バスを特定するバスＩＤと前記受信先バス内で前記受信先機器を特定するノードＩＤとの組合せから、前記送信元バスを特定するバスＩＤと前記送信元バス内で前記バスブリッジ自身を特定するノードＩＤとの組合せに付け替え、前記暗号化鍵および認証の手続きに関するパケットを前記受信先機器へ送信する際、前記暗号化鍵および認証の手続きに関するパケットの受信先の識別子であるディスティネーションＩＤを、前記送信元バスを特定するバスＩＤと前記送信元バス内で前記バスブリッジ自身を特定するノードＩＤとの組合せから、前記受信先バスを特定するバスＩＤと前記受信先バス内で前記受信先機器を特定するノードＩＤとの組合せに付け替え、前記暗号化鍵および認証の手続きに関するパケットの送信元の識別子であるソースＩＤを、前記送信元バスを特定するバスＩＤと前記送信元バス内で前記送信元機器を特定するノードＩＤとの組合せから、前記受信先バスを特定するバスＩＤと前記受信先バス内で前記バスブリッジ自身を特定するノードＩＤとの組合せに付け替える第２のＩＤ付替手段とを備えることを特徴とする第１の本発明のバスブリッジである。

【００２４】また、第３の本発明（請求項４に記載の本発明に対応）は、前記ストリームのデータが、暗号化鍵により暗号化されて送信される場合、前記受信先機器からの前記ストリームに対応する認証要求および認証の手続きに関するパケットを前記送信元機器へ送信する認証要求送受信手段と、前記送信元機器から前記ストリームに対応する前記暗号化鍵および認証の手続きに関するパケットを受信して前記受信先機器へ送信する暗号化鍵送受信手段と、前記送信元機器から、前記ストリームに対応し、前記暗号化鍵によって暗号化された前記データを受信して前記受信先機器へ送信するデータ送受信手段と、前記送信元バスおよび前記送信元機器を特定できる送信元識別子を、前記データ用パケットの所定の位置に書き込む識別子書込手段とを備え、前記受信先機器が、前記データ用パケットから前記送信元識別子を読み取り、前記認証要求および認証の手続きに関するパケットの所定の位置に、前記受信先バスおよび前記受信先機器自身を特定できる受信先識別子および前記送信元識別子

を書き込んで送信し、前記認証要求送受信手段が、前記認証要求および認証の手続きに関するパケットを受信して、前記送信元識別子を読み取り、これに基づいて、前記認証要求および認証の手続きに関するパケットを前記送信元機器へ送信し、前記送信元機器が、前記認証要求および認証の手続きに関するパケットを受信して、前記送信元識別子を読み取り、前記暗号化鍵および認証の手続きに関するパケットの所定の位置に、前記送信元識別子および前記受信先識別子を書き込んで送信し、前記暗号化鍵送受信手段が、前記暗号化鍵および認証の手続きに関するパケットを受信して、前記受信先識別子を読み取り、これに基づいて、前記暗号化鍵および認証の手続きに関するパケットを前記受信先機器へ送信することを特徴とする第１の本発明のバスブリッジである。

【００２５】また、第４の本発明（請求項６に記載の本発明に対応）は、前記ストリームのデータが、暗号化鍵により暗号化されて送信される場合、前記送信元機器および前記受信先機器とそれぞれ前記ストリームに対応する認証を行う認証手段と、前記送信元機器から受け渡された、前記ストリームに対応する前記暗号化鍵を保持し、これを、前記受信先機器からの要求に応じて、前記受信先機器へ送信する暗号化鍵保持手段とを備えることを特徴とする第１の本発明のバスブリッジである。

【００２６】また、第５の本発明（請求項９に記載の本発明に対応）は、前記ストリームのデータが、暗号化鍵により暗号化されて送信される場合、前記送信元機器および前記受信先機器とそれぞれ前記ストリームに対応する認証を行う認証手段と、前記データを前記暗号化鍵によって解読する暗号解読手段と、前記解読されたデータをブリッジ用鍵によって再暗号化する再暗号化手段と、前記送信元機器から、前記ストリームに対応する前記暗号化鍵、および、前記暗号化鍵によって暗号化された前記ストリームに対応する前記データを受信する受信手段と、前記ブリッジ用鍵と前記再暗号化されたデータとを前記受信先機器へ送信する送信手段とを備えることを特徴とする第１の本発明のバスブリッジである。

【００２７】また、第６の本発明（請求項１５に記載の本発明に対応）は、本発明のバスブリッジの各手段の機能の全部または一部をコンピュータに実行させるプログラムを格納することを特徴とする記録媒体である。

【００２８】

【発明の実施の形態】以下に、本発明の実施の形態を図面を参照して説明する。

【００２９】（第１の実施の形態）まず、本発明の第１の実施の形態を図面を参照して説明する。

【００３０】図１は、本発明の第１の実施の形態におけるバスブリッジの構成を示す構成図である。本実施の形態におけるバスブリッジは、図６でおしたバスブリッジ１００と同様に、２つのＩＥＥＥ１３９４バスが接続されたバスブリッジである。

【００３１】図１に示すように、本実施の形態におけるバスブリッジ１０は、バス１と直接データの転送を行うＤ－Ｉ／Ｆ（ディジタルインターフェイス）１１と、バス２と直接データの伝達を行うＤ－Ｉ／Ｆ１２と、各バスから送信されてきたパケットに対してクロック調整処理等の従来のバスブリッジと同様の処理を行う主処理手段１３と、ＡＶプロトコルに準拠したアイソクロノスパケットのソースＩＤを付け替えるソースＩＤ付替手段１４（本発明の「ＩＤ付替手段」に対応）とで構成されている。なお、バス１、バス２には、図６と同様に、それぞれ複数の機器１０１、１０２、１０３、複数の機器２０１、２０２、２０３、・・・が接続されている（図示省略）。また、各機器およびバスブリッジに割り当てられているノードＩＤは、図６と同じとする。

【００３２】次に、本実施の形態におけるバスブリッジの動作を、データ送信元の機器およびデータ受信先の機器の動作とともに説明する。ここで送信元の機器がバス１に接続された機器１０３であり、受信側の機器がバス２に接続された機器２０２である場合を例として説明する。

【００３３】まず、機器１０３は、図５で示したフォーマットのアイソクロノスパケットに実データおよび必要な情報を書き込んで、バス１へ出力する。このとき、当該アイソクロノスパケット中のソースＩＤ９０６には、バス１内で機器１０３を特定するための識別子であるノードＩＤ「３」が書き込まれている。

【００３４】バスブリッジ１０の主処理手段１３は、Ｄ－Ｉ／Ｆ１１を介して、機器１０３が出力したアイソクロノスパケットをバス１から受け取り、クロック調整等の処理を行う。このとき、ソースＩＤ付替手段１４は、当該アイソクロノスパケット中のソースＩＤ９０６に書き込まれている、機器１０３のノードＩＤ「３」を、バス２内でバスブリッジ１０を特定するための識別子であるノードＩＤ「４」に付け替える。ソースＩＤ付替手段１４によるソースＩＤの付け替え、および、主処理手段１３が行われると、当該アイソクロノスパケットは、Ｄ－Ｉ／Ｆ１２を介して、バス２へ出力される。

【００３５】機器２０２は、バス２へ出力されたアイソクロノスパケットを受信し、ソースＩＤ９０６に書き込まれているノードＩＤ「４」により、当該アイソクロノスパケットがバスブリッジ１０から出力されたもの、すなわち、バス２以外のバスから送信されてきたものであることを判別できる。

【００３６】また、ソースＩＤ付替手段１４が上記ソースＩＤの付け替えを送信元のバスおよび受信先のバスと関連づけて記憶する機能を有しておれば、バス２にバス１から転送されるデータのストリーム数が、ＥＭＩの各暗号化モード毎に１つ以下の場合は、機器２０２は、当該アイソクロノスパケットの送信元の機器１０３への別のデータ等の送信を、バスブリッジ１０を介して行うこ

とができる。なお、バスブリッジ１０がバス２においてバスブリッジ自身を特定するノードＩＤを複数個有している場合は、当該ノードＩＤ毎に前記ストリーム数が、ＥＭＩの各暗号化モード毎に１つ以下の場合において、機器２０２は、当該アイソクロノスパケットの送信元の機器１０３への別のデータ等の送信を、バスブリッジ１０を介して行うことができる。

【００３７】以上により、本実施の形態におけるバスブリッジは、ＡＶプロトコルに準拠したアイソクロノスパケットのような単一バス内でのみ送信元の機器を特定できるようなデータパケットによるデータ転送を、異なるバス間にまたがって行う場合において、受信先の機器が間接的に送信元の機器を判別できるものであることがわかる。

【００３８】（第２の実施の形態）次に、本発明の第２の実施の形態を図面を参照して説明する。

【００３９】図２は、本発明の第２の実施の形態におけるバスブリッジの構成を示す構成図である。本実施の形態におけるバスブリッジは、第１の実施の形態におけるバスブリッジと同様に、２つのＩＥＥＥ１３９４バスが接続されたバスブリッジである。したがって、本実施の形態において、特に説明のないものについては、第１の実施の形態と同じとし、第１の実施の形態と同一符号を付与している構成部材については、特に説明のない限り、第１の実施の形態と同様の機能を持つものとする。

【００４０】図２に示すように、本実施の形態におけるバスブリッジ２０が、図１で示した第１の実施の形態におけるバスブリッジ１０と異なるのは、本発明の「第２のＩＤ付替手段」の機能を有するＩＤ付替手段２１を備えている点である。なお、Ｄ－Ｉ／Ｆ１１、１２は、本発明の「認証要求送受信手段」、「暗号化鍵送受信手段」および「データ送受信手段」の機能を有するものである。

【００４１】次に、本実施の形態におけるバスブリッジの動作を、データ送信元の機器およびデータ受信先の機器の動作とともに説明する。第１の実施の形態と同様に、送信元の機器がバス１に接続された機器１０３であり、受信側の機器がバス２に接続された機器２０２である場合を例として説明する。

【００４２】まず、機器１０３は、データ暗号化鍵Ｋｃによって実データを暗号化し、図５で示したフォーマットのアイソクロノスパケットに暗号化された実データおよび必要な情報を書き込んで、バス１へ出力する。このとき、当該アイソクロノスパケット中のソースＩＤ９０６には、バス１内で機器１０３を特定するための識別子であるノードＩＤ「３」が書き込まれている。なお、データ暗号化鍵Ｋｃは、定期的または不定期的に更新生成されるものとする。

【００４３】バスブリッジ２０の主処理手段１３は、Ｄ－Ｉ／Ｆ１１を介して、機器１０３が出力したアイソクロノスパケットをバス１から受け取り、クロック調整等の処理を行う。このとき、ソースＩＤ付替手段１４は、当該アイソクロノスパケット中のソースＩＤ９０６に書き込まれている、機器１０３のノードＩＤ「３」を、バス２内でバスブリッジ２０を特定するための識別子であるノードＩＤ「４」に付け替える。ソースＩＤ付替手段１４によるソースＩＤの付け替え、および、主処理手段１３が行われると、当該アイソクロノスパケットは、Ｄ－Ｉ／Ｆ１２を介して、バス２へ出力される。

【００４４】機器２０２は、バス２へ出力されたアイソクロノスパケットを受信し、当該アイソクロノスパケット中のＳｙフィールド９１０に格納されているＥＭＩ値を読み取り、これが「１０」または「１１」である場合には、当該アイソクロノスパケット中の実データが暗号化されているものであると判断して、ソースＩＤ９０６に書き込まれているノードＩＤ「４」により、当該アイソクロノスパケットがバスブリッジ２０から出力されたもの、すなわち、バス２以外のバスから送信されてきたものであることを判別し、実データの解読のために、当該アイソクロノスパケットの送信元（見掛け上はバスブリッジ２０、実際は機器１０３）に対して、認証要求および認証の手続きに関するエイシンクロナスパケットを送信する（バス２へ出力する）。このとき、当該エイシンクロナスパケット中のディスティネーションＩＤには、バス２を特定するための識別子であるバスＩＤ（例えば、「２」）と、バス２内でバスブリッジ２０を特定するための識別子であるノードＩＤ「４」とが書き込まれており、当該エイシンクロナスパケット中のソースＩＤには、バス２を特定するための識別子であるバスＩＤ「２」と、バス２内で機器２０２を特定するための識別子であるノードＩＤ「２」とが書き込まれている。

【００４５】バスブリッジ２０の主処理手段１３は、Ｄ－Ｉ／Ｆ１２を介して、機器２０２が出力した認証要求および認証の手続きに関するエイシンクロナスパケットをバス２から受け取り、Ｄ－Ｉ／Ｆ１１を介して、バス１へ出力する。この間に、ＩＤ付替手段２１は、当該エイシンクロナスパケット中のディスティネーションＩＤを、バス２のバスＩＤ「２」とバス２内でのバスブリッジ２０のノードＩＤ「４」との組合せから、バス１のバスＩＤ（例えば、「１」）と機器１０３のノードＩＤ「３」との組合せに付け替え、当該エイシンクロナスパケット中のソースＩＤを、バス２のバスＩＤ「２」と機器２０２のノードＩＤ「２」との組合せから、バス１のバスＩＤ「１」とバス１内でのバスブリッジ２０のノードＩＤ「０」との組合せに付け替える。機器１０３は、バス１へ出力された認証要求および認証の手続きに関するエイシンクロナスパケットを受信し、認証を行い、当該エイシンクロナスパケット中のソースＩＤから当該エイシンクロナスパケットの送信元（見掛け上はバスブリッジ２０、実際は機器２０２）を判別し、鍵交換用鍵Ｋ

ｘによってデータ暗号化鍵Ｋｃを暗号化し、暗号化されたデータ暗号化鍵Ｋｃおよび鍵交換用鍵Ｋｘをそれぞれ異なる暗号化鍵および認証の手続きに関するエイシンクロナスパケット（以下、それぞれ「Ｋｃ用エイシンクロナスパケット」、「Ｋｘ用エイシンクロナスパケット」と記す）に書き込んで、バス１へ出力する。このとき、当該Ｋｃ用エイシンクロナスパケットおよびＫｘ用エイシンクロナスパケット中のディスティネーションＩＤには、バス１のバスＩＤ「１」と、バス１内でのバスブリッジ２０のノードＩＤ「０」とが書き込まれており、当該Ｋｃ用エイシンクロナスパケットおよびＫｘ用エイシンクロナスパケット中のソースＩＤには、バス１のバスＩＤ「１」と、機器１０３のノードＩＤ「３」とが書き込まれている。なお、上述したように、データ暗号化鍵Ｋｃは、定期的または不定期的に更新生成されるものなので、機器１０３は、データ暗号化鍵Ｋｃｎを更新生成する度に、鍵交換用鍵Ｋｘによって新しいデータ暗号化鍵Ｋｃｎを暗号化し、暗号化された新しいデータ暗号化鍵Ｋｃｎを別の暗号化鍵および認証の手続きに関するエイシンクロナスパケットに書き込んで、鍵の要求に応じてバス１へ出力する。

【００４６】バスブリッジ２０の主処理手段１３は、Ｄ－Ｉ／Ｆ１１を介して、機器１０３が出力したＫｃ用エイシンクロナスパケットおよびＫｘ用エイシンクロナスパケットをバス１から受け取り、Ｄ－Ｉ／Ｆ１２を介して、バス２へ出力する。この間に、ＩＤ付替手段２１は、当該Ｋｃ用エイシンクロナスパケットおよびＫｘ用エイシンクロナスパケット中のディスティネーションＩＤを、バス１のバスＩＤ「１」とバス１内でのバスブリッジ２０のノードＩＤ「０」との組合せから、バス２のバスＩＤ「２」と機器２０２のノードＩＤ「２」との組合せに付け替え、当該Ｋｃ用エイシンクロナスパケットおよびＫｘ用エイシンクロナスパケット中のソースＩＤを、バス１のバスＩＤ「１」と機器１０３のノードＩＤ「３」との組合せから、バス２のバスＩＤ「２」とバス２内でのバスブリッジ２０のノードＩＤ「４」との組合せに付け替える。なお、暗号化された新しいデータ暗号化鍵Ｋｃｎが書き込まれた別の暗号化鍵および認証の手続きに関するエイシンクロナスパケットについても、上記と同様の処理を行う。

【００４７】機器２０２は、バス２へ出力されたＫｃ用エイシンクロナスパケットおよびＫｘ用エイシンクロナスパケットを受信し、当該Ｋｃ用エイシンクロナスパケットおよびＫｘ用エイシンクロナスパケット中のソースＩＤに書き込まれているノードＩＤ「４」により、当該Ｋｃ用エイシンクロナスパケットおよびＫｘ用エイシンクロナスパケットがバスブリッジ２０から出力されたもの、すなわち、バス２以外のバスから送信されてきたものであることを判別する。そして、得られた鍵交換用鍵Ｋｘによってデータ暗号化鍵Ｋｃを解読し、解読されたデータ暗号化鍵Ｋｃによって実データを解読する。一度データ暗号化鍵Ｋｃを入手すると、それ以降に送信されてくるアイソクロノスパケットの実データの解読については、新しいデータ暗号化鍵Ｋｃｎが別の暗号化鍵および認証の手続きに関するエイシンクロナスパケットによって送信されてくるまで、同一のデータ暗号化鍵Ｋｃによって行う。

【００４８】以上により、本実施の形態におけるバスブリッジは、ＡＶプロトコルに準拠したアイソクロノスパケットのような単一バス内でのみ送信元の機器を特定できるようなデータパケットによるデータ転送を、異なるバス間にまたがって行う場合において、受信先の機器が間接的に送信元の機器を判別できるものであることがわかる。

【００４９】また、本実施の形態におけるバスブリッジは、前記アイソクロノスパケットの受信先バス内でバスブリッジ自身を特定するノードＩＤ１つに対して、前記受信先バスに前記受信先バス以外の前記バスから転送されるストリーム数が、ＥＭＩの各暗号化モード毎に１つ以下の場合は、実データが暗号化されて送信される場合、前記アイソクロノスパケットの送信元の機器と受信先の機器との間での認証・鍵交換が確実に行われるものであることがわかる。言い換えれば、バスブリッジが前記ストリーム数を上記条件に制限する機能を有しておれば、常に、前記アイソクロノスパケットの送信元の機器と受信先の機器との間での認証・鍵交換が確実に行われるものであることがわかる。

【００５０】なお、本実施の形態においては、本発明の暗号化鍵が、定期的または不定期的に更新生成されるデータ暗号化鍵と、前記データ暗号化鍵の暗号化に用いる鍵交換用鍵とで構成されるとして説明したが、データ暗号化鍵のみで構成される場合は、データ暗号化鍵は暗号化されずに送信され、鍵交換鍵の送信は行われない。

【００５１】また、本実施の形態におけるバスブリッジ２０のＩＤ付替手段２１の替わりに、送信元バスおよび送信元機器を特定できる送信元識別子を、アイソクロノスパケットの所定の位置に書き込む識別子書込手段を備えるバスブリッジとすると、受信先機器が、前記アイソクロノスパケットから前記送信元識別子を読み取り、認証要求および認証の手続きに関するエイシンクロナスパケットの所定の位置に、受信先バスおよび前記受信先機器自身を特定できる受信先識別子および前記送信元識別子を書き込んで送信し、Ｄ－Ｉ／Ｆ１１、１２が、前記認証要求および認証の手続きに関するエイシンクロナスパケットを受信して、前記送信元識別子を読み取り、これに基づいて、前記認証要求および認証の手続きに関するエイシンクロナスパケットを前記送信元機器へ送信し、前記送信元機器が、前記認証要求および認証の手続きに関するエイシンクロナスパケットを受信して、前記送信元識別子を読み取り、暗号化鍵および認証の手続き

17

に関するエイシンクロナスパケットの所定の位置に、前記送信元識別子および前記受信先識別子を書き込んで送信し、Ｄ－Ｉ／Ｆ１１、１２が、前記暗号化鍵および認証の手続きに関するエイシンクロナスパケットを受信して、前記受信先識別子を読み取り、これに基づいて、前記暗号化鍵および認証の手続きに関するエイシンクロナスパケットを前記受信先機器へ送信することによって、ＡＶプロトコルに準拠したアイソクロノスパケットのような単一バス内でのみ送信元の機器を特定できるようなデータパケットによるデータ転送を、異なるバス間にまたがって行う場合において、受信先の機器が直接送信元の機器を判別でき、その上、ストリーム数に関わらず、常に、アイソクロノスパケットの送信元の機器と受信先の機器との間での認証・鍵交換が確実に行われる。アイソクロノスパケットの所定の位置については、例えば、図５のフォーマット中で各転送に直接関係のない位置を選定して仮想的に送信元識別子を書き込むことになるが、エイシンクロナスパケットの所定の位置については、アイソクロノスパケットと同様に選定してもよいし、エイシンクロナスパケットのソースＩＤおよびディスティネーションＩＤの位置としてもよい。

【００５２】（第３の実施の形態）次に、本発明の第３の実施の形態を図面を参照して説明する。

【００５３】図３は、本発明の第３の実施の形態におけるバスブリッジの構成を示す構成図である。本実施の形態におけるバスブリッジは、第１の実施の形態におけるバスブリッジと同様に、２つのＩＥＥＥ１３９４バスが接続されたバスブリッジである。したがって、本実施の形態において、特に説明のないものについては、第１の実施の形態と同じとし、第１の実施の形態と同一符号を付与している構成部材については、特に説明のない限り、第１の実施の形態と同様の機能を持つものとする。

【００５４】図３に示すように、本実施の形態におけるバスブリッジ３０が、図１で示した第１の実施の形態におけるバスブリッジ１０と異なるのは、本発明の「認識手段」の機能を有する認識手段３１と、本発明の「暗号化鍵保持手段」の機能を有する暗号化鍵保持手段３２とを備えている点である。なお、認証手段３１は、データの転送要求をしてきた装置（例えば、機器２０２）との間で、バスブリッジ３０およびその装置が正規の装置であるかどうかを互いに確かめ合うため、所定の秘密関数を利用して認証作業を行い、その結果として、認証相手に対応したサブキーを生成する手段である。

【００５５】次に、本実施の形態におけるバスブリッジの動作を、データ送信元の機器およびデータ受信先の機器の動作とともに説明する。第１の実施の形態と同様に、送信元の機器がバス１に接続された機器１０３であり、受信側の機器がバス２に接続された機器２０２である場合を例として説明する。

【００５６】まず、機器１０３は、データ暗号化鍵Ｋｃ

18

によって実データを暗号化し、図５で示したフォーマットのアイソクロノスパケットに暗号化された実データおよび必要な情報を書き込んで、バス１へ出力する。このとき、当該アイソクロノスパケット中のソースＩＤ９０６には、バス１内で機器１０３を特定するための識別子であるノードＩＤ「３」が書き込まれている。なお、データ暗号化鍵Ｋｃは、定期的または不定期的に更新生成されるものとする。

【００５７】バスブリッジ３０の主処理手段１３は、Ｄ－Ｉ／Ｆ１１を介して、機器１０３が出力したアイソクロノスパケットをバス１から受け取り、クロック調整等の処理を行う。このとき、ソースＩＤ付替手段１４は、当該アイソクロノスパケット中のソースＩＤ９０６に書き込まれている、機器１０３のノードＩＤ「３」を、バス２内でバスブリッジ３０を特定するための識別子であるノードＩＤ「４」に付け替える。ソースＩＤ付替手段１４によるソースＩＤの付け替え、および、主処理手段１３が行われると、当該アイソクロノスパケットは、Ｄ－Ｉ／Ｆ１２を介して、バス２へ出力される。この間に、認証手段３１は、当該アイソクロノスパケット中のＳｙフィールド９１０に格納されているＥＭＩ値を読み取り、これが「１０」または「１１」である場合には、当該アイソクロノスパケット中の実データが暗号化されているものであると判断して、当該アイソクロノスパケットの送信元である機器１０３に対して、認証要求および認証の手続きに関するエイシンクロナスパケットをＤ－Ｉ／Ｆ１１、バス１を介して送信する。このとき、当該エイシンクロナスパケット中のディスティネーションＩＤには、バス１のバスＩＤ「１」と、機器１０３のノードＩＤ「３」とが書き込まれており、当該エイシンクロナスパケット中のソースＩＤには、バス１のバスＩＤ「１」と、バス１内でのバスブリッジ３０のノードＩＤ「０」とが書き込まれている。

【００５８】機器１０３は、認証手段３１からバス１へ出力された認証要求および認証の手続きに関するエイシンクロナスパケットを受信し、認証を行い、当該エイシンクロナスパケット中のソースＩＤから当該エイシンクロナスパケットの送信元（バスブリッジ３０）を判別し、鍵交換用鍵Ｋｘによってデータ暗号化鍵Ｋｃを暗号化し、暗号化されたデータ暗号化鍵Ｋｃおよび鍵交換用鍵Ｋｘを、それぞれＫｃ用エイシンクロナスパケット、Ｋｘ用エイシンクロナスパケットに書き込んで、鍵の要求に応じてバス１へ出力する。このとき、当該Ｋｃ用エイシンクロナスパケットおよびＫｘ用エイシンクロナスパケット中のディスティネーションＩＤには、バス１のバスＩＤ「１」と、バス１内でのバスブリッジ３０のノードＩＤ「０」とが書き込まれており、当該エイシンクロナスパケット中のソースＩＤには、バス１のバスＩＤ「１」と、機器１０３のノードＩＤ「３」とが書き込まれている。なお、上述したように、データ暗号化鍵Ｋｃ

は、定期的または不定期的に更新生成されるものなので、機器１０３は、データ暗号化鍵Ｋｃｎを更新生成する度に、鍵交換用鍵Ｋｘによって新しいデータ暗号化鍵Ｋｃｎを暗号化し、暗号化された新しいデータ暗号化鍵Ｋｃｎを別の暗号化鍵および認証の手続きに関するエイシンクロナスパケットに書き込んで、鍵の要求に応じてバス１へ出力する。

【００５９】一方、機器２０２は、バス２へ出力されたアイソクロノスパケットを受信し、当該アイソクロノスパケット中のＳｙフィールド９１０に格納されているＥＭＩ値を読み取り、これが「１０」または「１１」である場合には、当該アイソクロノスパケット中の実データが暗号化されているものであると判断して、ソースＩＤ９０６に書き込まれているノードＩＤ「４」により、当該アイソクロノスパケットがバスブリッジ３０から出力されたものであることを判別し、実データの解読のために、当該アイソクロノスパケットの送信元（バスブリッジ３０）に対して、認証要求および認証の手続きに関するエイシンクロナスパケットを送信する（バス２へ出力する）。このとき、当該エイシンクロナスパケット中のディスティネーションＩＤには、バス２のバスＩＤ「２」と、バス２内でのバスブリッジ３０のノードＩＤ「４」とが書き込まれており、当該エイシンクロナスパケット中のソースＩＤには、バス２のバスＩＤ「２」と、機器２０２のノードＩＤ「２」とが書き込まれている。

【００６０】バスブリッジ３０の認証手段３１は、Ｄ－Ｉ／Ｆ１１を介して、機器１０３が出力したＫｃ用エイシンクロナスパケットおよびＫｘ用エイシンクロナスパケットをバス１から受け取り、認証を行う。認証が完了すると、暗号化鍵保持手段３２は、これらのエイシンクロナスパケットから、暗号化されたデータ暗号化鍵Ｋｃおよび鍵交換用鍵Ｋｘを取り出して保持する。そして、Ｄ－Ｉ／Ｆ１２を介して、機器２０２が出力した認証要求および認証の手続きに関するエイシンクロナスパケットをバス２から受信すると、認証手段３１は、認証を行う。認証が完了すると、Ｄ－Ｉ／Ｆ１２は、鍵の要求に応じて暗号化鍵保持手段３２が保持していた暗号化されたデータ暗号化鍵Ｋｃおよび鍵交換用鍵Ｋｘを、それぞれ異なる暗号化鍵および認証の手続きに関するエイシンクロナスパケット（以下、「新たなＫｃ用エイシンクロナスパケット」および「新たなＫｘ用エイシンクロナスパケット」と記す）に書き込んで、主処理手段１３によるクロック調整等の処理を行った後、バス２へ出力する。このとき、当該Ｋｃ用エイシンクロナスパケットおよびＫｘ用エイシンクロナスパケット中のディスティネーションＩＤには、バス２のバスＩＤ「２」と、機器２０２のノードＩＤ「２」とが書き込まれており、当該エイシンクロナスパケット中のソースＩＤには、バス２のバスＩＤ「２」と、バス２内でのバスブリッジ３０のノードＩＤ「４」とが書き込まれている。なお、暗号化された新しいデータ暗号化鍵Ｋｃｎについても、上記の暗号化されたデータ暗号化鍵Ｋｃと同様の処理を行う。

【００６１】機器２０２は、バス２へ出力されたＫｃ用エイシンクロナスパケットおよびＫｘ用エイシンクロナスパケットを受信し、当該Ｋｃ用エイシンクロナスパケットおよびＫｘ用エイシンクロナスパケット中のソースＩＤに書き込まれているノードＩＤ「４」により、当該Ｋｃ用エイシンクロナスパケットおよびＫｘ用エイシンクロナスパケットがバスブリッジ３０から出力されたものであることを判別する。そして、得られた鍵交換用鍵Ｋｘによってデータ暗号化鍵Ｋｃを解読し、解読されたデータ暗号化鍵Ｋｃによって実データを解読する。一度データ暗号化鍵Ｋｃを入手すると、それ以降に送信されてくるアイソクロノスパケットの実データの解読については、新しいデータ暗号化鍵Ｋｃｎが別の暗号化鍵および認証の手続きに関するエイシンクロナスパケットによって送信されてくるまで、同一のデータ暗号化鍵Ｋｃによって行う。

【００６２】以上により、本実施の形態におけるバスブリッジは、ＡＶプロトコルに準拠したアイソクロノスパケットのような単一バス内でのみ送信元の機器を特定できるようなデータパケットによるデータ転送を、異なるバス間にまたがって行う場合において、受信先の機器が間接的に送信元の機器を判別できるものであることがわかる。

【００６３】また、本実施の形態におけるバスブリッジは、前記アイソクロノスパケットの受信先バス内でバスブリッジ自身を特定するノードＩＤ１つに対して、前記受信先バスに前記受信先バス以外の前記バスから転送されるストリーム数が、ＥＭＩの各暗号化モード毎に１つ以下の場合は、実データが暗号化されて送信される場合、前記アイソクロノスパケットの送信元の機器と受信先の機器との間での認証・鍵交換が確実に行われるものであることがわかる。言い換えれば、バスブリッジが前記ストリーム数を上記条件に制限する機能を有しておれば、常に、前記アイソクロノスパケットの送信元の機器と受信先の機器との間での認証・鍵交換が確実に行われるものであることがわかる。

【００６４】なお、本実施の形態においては、本発明の暗号化鍵が、定期的または不定期的に更新生成されるデータ暗号化鍵と、前記データ暗号化鍵の暗号化に用いる鍵交換用鍵とで構成されるとして説明したが、データ暗号化鍵のみで構成される場合は、データ暗号化鍵は暗号化されずに送信され、鍵交換鍵の送信は行われない。

【００６５】（第４の実施の形態）次に、本発明の第４の実施の形態を図面を参照して説明する。

【００６６】図４は、本発明の第４の実施の形態におけるバスブリッジの構成を示す構成図である。本実施の形態におけるバスブリッジは、第１の実施の形態における

21

バスブリッジと同様に、２つのＩＥＥＥ１３９４バスが接続されたバスブリッジである。したがって、本実施の形態において、特に説明のないものについては、第１の実施の形態と同じとし、第１の実施の形態と同一符号を付与している構成部材については、特に説明のない限り、第１の実施の形態と同様の機能を持つものとする。

【００６７】図４に示すように、本実施の形態におけるバスブリッジ４０が、図１で示した第１の実施の形態におけるバスブリッジ１０と異なるのは、本発明の「認識手段」の機能を有する認識手段３１（第３の実施の形態で説明した認識手段３１と同じもの）と、本発明の「暗号解読手段」の機能を有する暗号解読手段４１と、本発明の「再暗号化手段」の機能を有する再暗号化手段４２とを備えている点である。なお、Ｄ－Ｉ／Ｆ１１、１２は、本発明の「受信手段」および「送信手段」の機能を有するものである。

【００６８】次に、本実施の形態におけるバスブリッジの動作を、データ送信元の機器およびデータ受信先の機器の動作とともに説明する。第１の実施の形態と同様に、送信元の機器がバス１に接続された機器１０３であり、受信側の機器がバス２に接続された機器２０２である場合を例として説明する。

【００６９】まず、機器１０３は、データ暗号化鍵Ｋｃによって実データを暗号化し、図５で示したフォーマットのアイソクロノスパケットに暗号化された実データおよび必要な情報を書き込んで、バス１へ出力する。このとき、当該アイソクロノスパケット中のソースＩＤ９０６には、バス１内で機器１０３を特定するための識別子であるノードＩＤ「３」が書き込まれている。なお、データ暗号化鍵Ｋｃは、定期的または不定期的に更新生成されるものとする。

【００７０】バスブリッジ４０の認証手段３１は、当該アイソクロノスパケット中のＳｙフィールド９１０に格納されているＥＭＩ値を読み取り、これが「１０」または「１１」である場合には、当該アイソクロノスパケット中の実データが暗号化されているものであると判断して、当該アイソクロノスパケットの送信元である機器１０３に対して、認証要求および認証の手続きに関するエイシンクロナスパケットをＤ－Ｉ／Ｆ１１、バス１を介して送信する。このとき、当該エイシンクロナスパケット中のディスティネーションＩＤには、バス１のバスＩＤ「１」と、機器１０３のノードＩＤ「３」とが書き込まれており、当該エイシンクロナスパケット中のソースＩＤには、バス１のバスＩＤ「１」と、バス１内でのバスブリッジ４０のノードＩＤ「０」とが書き込まれている。

【００７１】機器１０３は、認証手段３１からバス１へ出力された認証要求および認証の手続きに関するエイシンクロナスパケットを受信し、認証を行い、当該エイシンクロナスパケット中のソースＩＤから当該エイシンクロナスパケットの送信元（バスブリッジ３０）を判別し、鍵交換用鍵Ｋｘによってデータ暗号化鍵Ｋｃを暗号化し、暗号化されたデータ暗号化鍵Ｋｃおよび鍵交換用鍵Ｋｘを、それぞれＫｃ用エイシンクロナスパケット、Ｋｘ用エイシンクロナスパケットに書き込んで、バス１へ出力する。このとき、当該Ｋｃ用エイシンクロナスパケットおよびＫｘ用エイシンクロナスパケット中のディスティネーションＩＤには、バス１のバスＩＤ「１」と、バス１内でのバスブリッジ４０のノードＩＤ「０」とが書き込まれており、当該エイシンクロナスパケット中のソースＩＤには、バス１のバスＩＤ「１」と、機器１０３のノードＩＤ「３」とが書き込まれている。なお、上述したように、データ暗号化鍵Ｋｃは、定期的または不定期的に更新生成されるものなので、機器１０３は、データ暗号化鍵Ｋｃｎを更新生成する度に、鍵交換用鍵Ｋｘによって新しいデータ暗号化鍵Ｋｃｎを暗号化し、暗号化された新しいデータ暗号化鍵Ｋｃｎを別の暗号化鍵および認証の手続きに関するエイシンクロナスパケットに書き込んで、鍵の要求に応じてバス１へ出力する。

22

【００７２】バスブリッジ４０の認証手段３１は、Ｄ－Ｉ／Ｆ１１を介して、機器１０３が出力したＫｃ用エイシンクロナスパケットおよびＫｘ用エイシンクロナスパケットをバス１から受け取り、認証を行う。認証が完了すると、暗号解読手段４１は、これらのエイシンクロナスパケットから、暗号化されたデータ暗号化鍵Ｋｃおよび鍵交換用鍵Ｋｘを取り出して、鍵交換用鍵Ｋｘによってデータ暗号化鍵Ｋｃを解読し、解読されたデータ暗号化鍵Ｋｃによって、既に受信されたアイソクロノスパケットから得られる暗号化された実データを解読する。再暗号化手段４２は、解読された実データを、自らが定期的または不定期的に更新生成するブリッジ用暗号化鍵Ｋｂｃによって再暗号化し、このブリッジ用暗号化鍵Ｋｂｃをブリッジ用鍵交換用鍵Ｋｂｘによって暗号化する。Ｄ－Ｉ／Ｆ１２は、再暗号化された実データをバス２へ送信するためのアイソクロノスパケットを図５で示したフォーマットに従って生成し、主処理手段１３によるクロック調整等の処理を行った後、バス２へ出力する。このとき、ソースＩＤ付替手段１４は、当該アイソクロノスパケット中のソースＩＤ９０６に、バス２内でバスブリッジ４０を特定するための識別子であるノードＩＤ「４」を書き込む。なお、暗号解読手段４１は、一度データ暗号化鍵Ｋｃを入手すると、それ以降に送信されてくるアイソクロノスパケットの実データの解読については、新しいデータ暗号化鍵Ｋｃｎが別の暗号化鍵および認証の手続きに関するエイシンクロナスパケットによって送信されてくるまで、同一のデータ暗号化鍵Ｋｃによって行う。それに対応して、再暗号化手段４２は、同一のブリッジ用暗号化鍵Ｋｂｃによって再暗号化を行い、新しいデータ暗号化鍵Ｋｃｎが送信されてくると、新し

いブリッジ用暗号化鍵Ｋｂｃｎに切り替えて、これによって再暗号化を行い、この新しいブリッジ用暗号化鍵Ｋｂｃｎをブリッジ用鍵交換用鍵Ｋｂｘによって暗号化する。

【００７３】機器２０２は、バス２へ出力されたアイソクロノスパケットを受信し、当該アイソクロノスパケット中のＳｙフィールド９１０に格納されているＥＭＩ値を読み取り、これが「１０」または「１１」である場合には、当該アイソクロノスパケット中の実データが暗号化されているものであると判断して、ソースＩＤ９０６に書き込まれているノードＩＤ「４」により、当該アイソクロノスパケットがバスブリッジ４０から出力されたものであることを判別し、実データの解読のために、当該アイソクロノスパケットの送信元（バスブリッジ４０）に対して、認証要求および認証の手続きに関するエイシンクロナスパケットを送信する（バス２へ出力する）。このとき、当該エイシンクロナスパケット中のディスティネーションＩＤには、バス２のバスＩＤ「２」と、バス２内でのバスブリッジ４０のノードＩＤ「４」とが書き込まれており、当該エイシンクロナスパケット中のソースＩＤには、バス２のバスＩＤ「２」と、機器２０２のノードＩＤ「２」とが書き込まれている。

【００７４】バスブリッジ４０の認証手段３１は、Ｄ－Ｉ／Ｆ１２を介して、機器２０２が出力した認証要求および認証の手続きに関するエイシンクロナスパケットをバス２から受信すると、認証を行う。認証が完了すると、Ｄ－Ｉ／Ｆ１２は、暗号化されたブリッジ用暗号化鍵Ｋｂｃおよびブリッジ用鍵交換用鍵Ｋｂｘを、それぞれ異なる暗号化鍵および認証の手続きに関するエイシンクロナスパケット（以下、「新たなＫｂｃ用エイシンクロナスパケット」および「新たなＫｂｘ用エイシンクロナスパケット」と記す）に書き込んで、鍵の要求に応じてバス２へ出力する。このとき、当該Ｋｂｃ用エイシンクロナスパケットおよびＫｂｘ用エイシンクロナスパケット中のディスティネーションＩＤには、バス２のバスＩＤ「２」と、機器２０２のノードＩＤ「２」とが書き込まれており、当該エイシンクロナスパケット中のソースＩＤには、バス２のバスＩＤ「２」と、バス２内でのバスブリッジ４０のノードＩＤ「４」とが書き込まれている。なお、ブリッジ用暗号化鍵Ｋｂｃが新しいブリッジ用暗号化鍵Ｋｂｃｎに切り替えられた場合において、新しいブリッジ用暗号化鍵Ｋｂｃｎの転送上の取扱いは、ブリッジ用暗号化鍵Ｋｂｃと同様である。

【００７５】機器２０２は、バス２へ出力されたＫｂｃ用エイシンクロナスパケットおよびＫｂｘ用エイシンクロナスパケットを受信し、当該Ｋｂｃ用エイシンクロナスパケットおよびＫｂｘ用エイシンクロナスパケット中のソースＩＤに書き込まれているノードＩＤ「４」により、当該Ｋｃ用エイシンクロナスパケットおよびＫｘ用エイシンクロナスパケットがバスブリッジ４０から出力されたものであることを判別する。そして、得られたブリッジ用鍵交換用鍵Ｋｂｘによってブリッジ用暗号化鍵Ｋｂｃを解読し、解読されたブリッジ用暗号化鍵Ｋｂｃによって実データを解読する。一度ブリッジ用暗号化鍵Ｋｂｃを入手すると、それ以降に送信されてくるアイソクロノスパケットの実データの解読については、新しいブリッジ用暗号化鍵Ｋｂｃｎが別の暗号化鍵および認証の手続きに関するエイシンクロナスパケットによって送信されてくるまで、同一のブリッジ用暗号化鍵Ｋｂｃによって行う。

【００７６】以上により、本実施の形態におけるバスブリッジは、ＡＶプロトコルに準拠したアイソクロノスパケットのような単一バス内でのみ送信元の機器を特定できるようなデータパケットによるデータ転送を、異なるバス間にまたがって行う場合において、受信先の機器が間接的に送信元の機器を判別できるものであることがわかる。

【００７７】また、本実施の形態におけるバスブリッジは、前記アイソクロノスパケットの受信先バスに前記受信先バス以外の前記バスから転送されるストリーム数に関わらず、実データが暗号化されて送信される場合、前記アイソクロノスパケットの送信元の機器と受信先の機器との間での認証・鍵交換が確実に行われるものであることがわかる。

【００７８】なお、本実施の形態においては、本発明の暗号化鍵が、定期的または不定期的に更新生成されるデータ暗号化鍵と、前記データ暗号化鍵の暗号化に用いる鍵交換用鍵とで構成され、本発明のブリッジ用鍵が、定期的または不定期的に更新生成されるブリッジ用暗号化鍵と、前記ブリッジ用暗号化鍵の暗号化に用いるブリッジ用鍵交換用鍵とで構成されるとして説明したが、本発明の暗号化鍵が、データ暗号化鍵のみで構成される場合は、本発明のブリッジ用鍵はブリッジ用暗号化鍵のみで構成され、データ暗号化鍵およびブリッジ用暗号化鍵は暗号化されずに送信され、鍵交換鍵およびブリッジ用鍵交換用鍵の送信は行われない。

【００７９】また、本実施の形態においては、本発明のブリッジ用暗号化鍵およびブリッジ用鍵交換用鍵は、バスブリッジが固有に生成したものであるとして説明したが、これに限らず、１つの送信元機器から送信されてくるストリームに対応するデータ暗号化鍵Ｋｃおよび／または鍵交換用鍵Ｋｘを、それぞれブリッジ用暗号化鍵Ｋｂｃおよび／またはブリッジ用鍵交換用鍵Ｋｂｘとして、当該ストリームに対応する解読・再暗号化の全部または一部を省略することができる。具体的には、以下の３ケースが想定される。

【００８０】１番目のケースは、ブリッジ用暗号化鍵Ｋｂｃおよびブリッジ用鍵交換用鍵Ｋｂｘが、１つのストリームに対応するデータ暗号化鍵Ｋｃおよび鍵交換用鍵Ｋｘとそれぞれ同じ場合である。この場合、このストリ

ームに対しては、ブリッジ用暗号化鍵Ｋｂｃと同じデータ暗号化鍵Ｋｃにより暗号化された実データと、ブリッジ用鍵交換用鍵Ｋｂｘと同じ鍵交換用鍵Ｋｘにより暗号化されたデータ暗号化鍵Ｋｂｃ（すなわち、Ｋｃ）は、暗号解読手段４１による解読および再暗号化手段４２による再暗号化を行われずに、機器２０２（受信先機器）へ送信される。他のストリームに対しては、本実施の形態において説明したのと同様に解読が行われ、ブリッジ用暗号化鍵Ｋｂｃ（すなわち、前記１つのストリームに対応するデータ暗号化鍵Ｋｃ）およびブリッジ用鍵交換用鍵Ｋｂｘ（すなわち、前記１つのストリームに対応する鍵交換用鍵Ｋｘ）によって、本実施の形態において説明したのと同様に実データ等の再暗号化が行われる。

【００８１】２番目のケースは、ブリッジ用暗号化鍵Ｋｂｃのみが、１つのストリームに対応するデータ暗号化鍵Ｋｃと同じ場合である。この場合、このストリームに対しては、Ｄ－Ｉ／Ｆ１１（本発明の受信手段）は、機器１０３（送信元機器）から、データ暗号化鍵Ｋｃによって暗号化された実データ、鍵交換用鍵Ｋｘによって暗号化されたデータ暗号化鍵Ｋｃおよび鍵交換用鍵Ｋｘを受信し、暗号解読手段４１は、データ暗号化鍵Ｋｃを鍵交換用鍵Ｋｘによって解読し、再暗号化手段４２は、データ暗号化鍵Ｋｃをブリッジ用暗号化鍵Ｋｂｃとし、これをバスブリッジ４０で生成されたブリッジ用鍵交換用鍵Ｋｂｘによって再暗号化する。このとき、暗号解読手段４１は実データの暗号化を行わず、したがって、再暗号化手段４２も実データの再暗号化は行わない。そして、Ｄ－Ｉ／Ｆ１２（本発明の送信手段）は、ブリッジ用鍵交換用鍵Ｋｂｃ、ブリッジ用鍵交換用鍵Ｋｂｘによって再暗号化されたブリッジ用暗号化鍵Ｋｂｃと、暗号解読手段４１による解読および再暗号化手段４２による再暗号化が行われなかった実データとを機器２０２（受信先機器）へ送信する。他のストリームに対しては、本実施の形態において説明したのと同様に解読が行われ、ブリッジ用暗号化鍵Ｋｂｃ（すなわち、前記１つのストリームに対応するデータ暗号化鍵Ｋｃ）およびブリッジ用鍵交換用鍵Ｋｂｘによって、本実施の形態において説明したのと同様に実データ等の再暗号化が行われる。

【００８２】３番目のケースは、ブリッジ用鍵交換用鍵Ｋｂｘのみが、１つのストリームに対応する鍵交換用鍵Ｋｘと同じ場合である。この場合、このストリームに対しては、Ｄ－Ｉ／Ｆ１１（本発明の受信手段）は、機器１０３（送信元機器）から、データ暗号化鍵Ｋｃによって暗号化された実データ、鍵交換用鍵Ｋｘによって暗号化されたデータ暗号化鍵Ｋｃおよび鍵交換用鍵Ｋｘを受信し、暗号解読手段４１は、データ暗号化鍵Ｋｃを鍵交換用鍵Ｋｘによって解読し、実データを解読されたデータ暗号化鍵Ｋｃによって解読する。再暗号化手段４２は、解読されたデータを、バスブリッジ４０で生成されたブリッジ用暗号化鍵Ｋｂｃによって再暗号化し、鍵交換用鍵Ｋｘをブリッジ用鍵交換用鍵Ｋｂｘとし、これによってブリッジ用暗号化鍵Ｋｘを再暗号化する。そして、Ｄ－Ｉ／Ｆ１２（本発明の送信手段）は、ブリッジ用鍵交換用鍵Ｋｂｃ、ブリッジ用鍵交換用鍵Ｋｂｘによって再暗号化されたブリッジ用暗号化鍵Ｋｂｃと、暗号解読手段４１による解読および再暗号化手段４２による再暗号化が行われなかった実データとを機器２０２（受信先機器）へ送信する。他のストリームに対しては、本実施の形態において説明したのと同様に解読が行われ、ブリッジ用暗号化鍵Ｋｂｃおよびブリッジ用鍵交換用鍵Ｋｂｘ（すなわち、前記１つのストリームに対応する鍵交換用鍵Ｋｘ）によって、本実施の形態において説明したのと同様に実データ等の再暗号化が行われる。

【００８３】なお、上述した第１～第４の実施の形態におけるバスブリッジは、２つのＩＥＥＥ１３９４バスが接続されたバスブリッジであるとして説明したが、これに限るものではなく、ＡＶプロトコルに準拠したアイソクロノスパケットのような単一バス内でのみ送信元の機器を特定できるようなデータパケットによるデータ転送を、異なるバス間にまたがって行うバスブリッジであればよい。接続するバスブリッジの数も２つに限らず、複数であればよい。３つ以上のバスが接続される場合であっても、１つのバスに他のバスからデータ転送が行われる場合の取扱いは、第１～第４の実施の形態において説明したのと同様である。

【００８４】また、上述した第１～第４の実施の形態においては、本発明のバスブリッジを中心に説明したが、本発明の記録媒体としては、以上説明した各手段の機能の全部または一部をコンピュータに実行させるプログラムを格納する記録媒体が挙げられる。

【００８５】

【発明の効果】以上説明したところから明らかなように、請求項１の本発明は、ＡＶプロトコルに準拠したアイソクロノスパケットのような単一バス内でのみ送信元の機器を特定できるようなデータパケットによるデータ転送を、異なるバス間にまたがって行う場合において、受信先の機器が直接または間接的に送信元の機器を判別できるバスブリッジを提供することができる。

【００８６】また、請求項２～１４の本発明は、請求項１の本発明の効果に加え、実データが暗号化されて送信される場合、前記送信元の機器と前記受信先の機器との間での認証・鍵交換が確実に行われるバスブリッジを提供することができる。

【００８７】また、請求項１５の本発明は、本発明のバスブリッジの各手段の機能の全部または一部をコンピュータに実行させるプログラムを格納する記録媒体を提供することができる。

【図面の簡単な説明】

【図１】本発明の第１の実施の形態におけるバスブリッジの構成を示す構成図である。

【図２】本発明の第２の実施の形態におけるバスブリッジの構成を示す構成図である。

【図３】本発明の第３の実施の形態におけるバスブリッジの構成を示す構成図である。

【図４】本発明の第４の実施の形態におけるバスブリッジの構成を示す構成図である。

【図５】ＡＶプロトコルに準拠したアイソクロノスパケットのフォーマットを示す図である。

【図６】バスブリッジによってデータ転送の仲介が行われる２つのＩＥＥＥ１３９４バスを示す概略構成図である。

【符号の説明】

１、２　バス

１０、２０、３０、４０、１００　バスブリッジ

１１、１２　Ｄ－Ｉ／Ｆ

１３　主処理手段

１４　ソースＩＤ付替手段

２１　ＩＤ付替手段

３１　認証手段

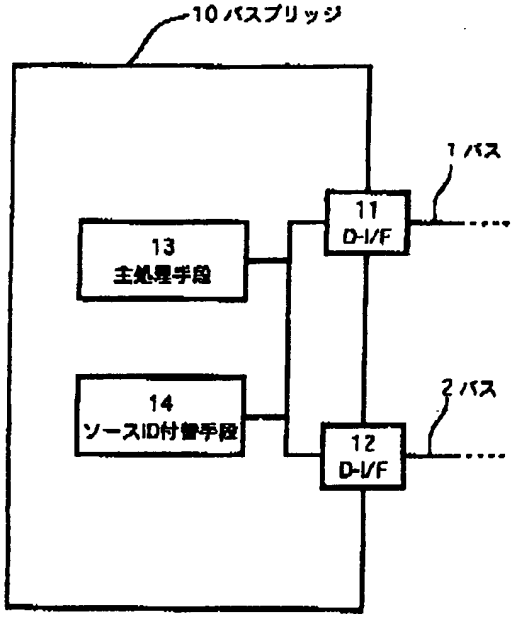
３２　暗号化鍵保持手段

４１　暗号解読手段

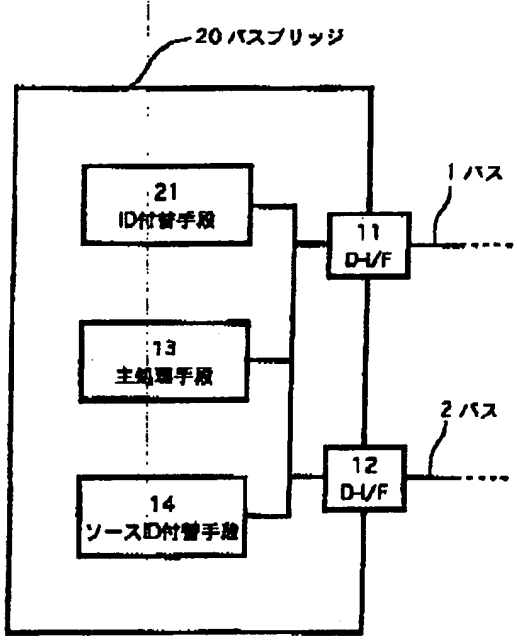
４２　再暗号化手段

１０１、１０２、１０３、２０１、２０２、２０３　機器

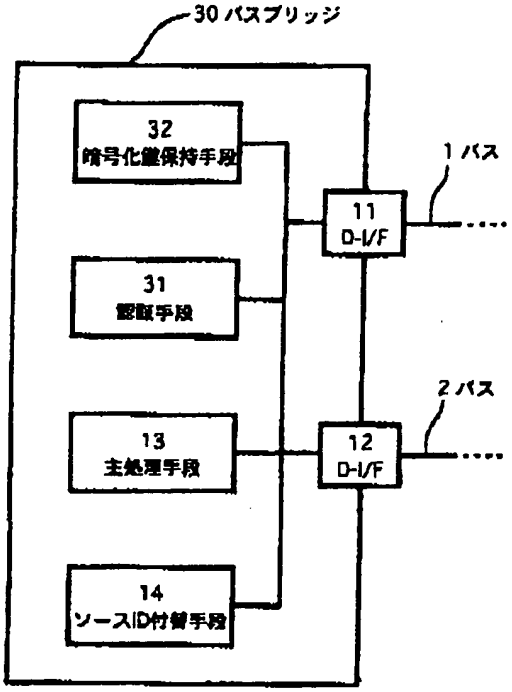
【図１】



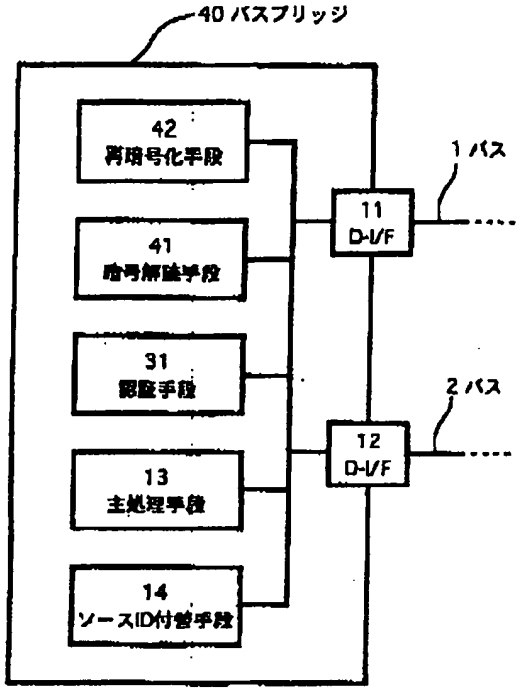
【図２】



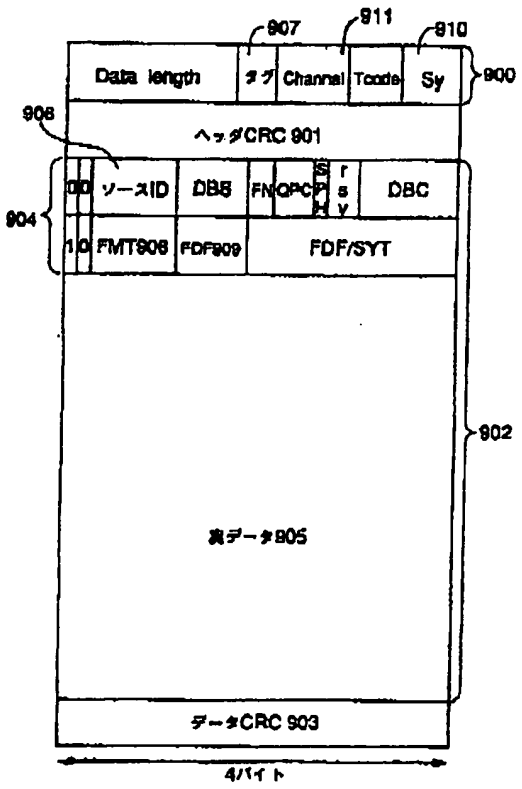
【図３】


30 バスブリッジ
32
暗号化鍵保持手段
31
認証手段
13
主処理手段
14
ソースID付替手段
11
D-I/F
12
D-I/F
1 バス
2 バス

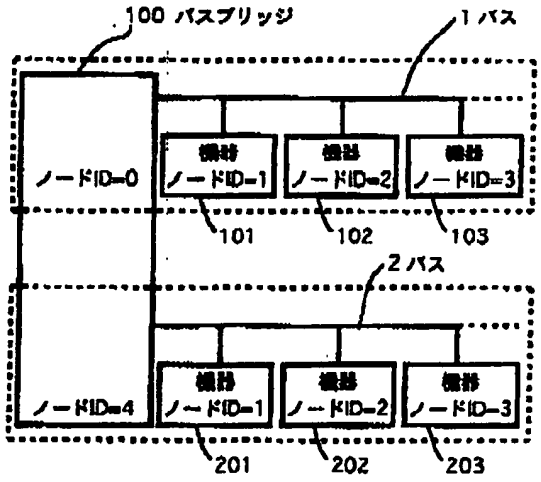
【図４】


40 バスブリッジ
42
再暗号化手段
41
暗号解読手段
31
認証手段
13
主処理手段
14
ソースID付替手段
11
D-I/F
12
D-I/F
1 バス
2 バス

【図５】


907
911
910
Data length
タグ
Channel
Tcode
Sy
900
908
ヘッダCRC 901
ソースID
DBS
FN
QPC
DBC
904
FMT906
FDF909
FDF/SYT
902
実データ905
データCRC 903
4バイト

【図６】


100 バスブリッジ
1 バス
ノードID=0
機器
ノードID=1
機器
ノードID=2
機器
ノードID=3
101
102
103
2 バス
ノードID=4
機器
ノードID=1
機器
ノードID=2
機器
ノードID=3
201
202
203

フロントページの続き

(72)発明者 西村 拓也
大阪府門真市大字門真1006番地 松下電器産業株式会社内
(72)発明者 武知 秀明
大阪府門真市大字門真1006番地 松下電器産業株式会社内
(72)発明者 久野 良樹
大阪府門真市大字門真1006番地 松下電器産業株式会社内
(72)発明者 浜本 康男
大阪府門真市大字門真1006番地 松下電器産業株式会社内

Fターム(参考) 5D044 DE49 GK17 HL11
5J104 AA07 KA02 KA04 PA07
5K033 AA08 CB01 CB09 CC01 CC04
DA13 DB18

Title of the Prior Art

Japanese Published Patent Application No. H12-165376

Date of Publication: June 16, 2000

Concise Statement of Relevancy

(1) Translation of paragraphs [0002]-[0013].

[0002]

[Background Art] Recently, high-speed serial bus interface (hereinafter described as 「IEEE1394 bus」 that employ IEEE 1394 specification (IEEE: THE INSTITUTE OF ELECTRICAL AND ELECTRINIC ENGINEERS, INC) has been paid attention; digital interface which play a large amount of data transfer in high speed and high quality.

[0003] As data transfer in IEEE 1394 specification, there are an isochronous communication which is suited to transfer of synchronous data such as video signal or audio signal as well as an asynchronous communication which is suited to transfer of asynchronous data such as control signals. Both of these communications can co-exist on IEEE1394bus.

[0004] The isochronous communication is a so-called communication of broadcast type, and isochronous packet which is output from a certain apparatus on IEEE1394 bus can be received by all of the apparatus connected on the bus.

[0005] On the other hand, asynchronous communication has both communication, one-to-one communication and broadcast-type communication. An asynchronous packet which is output from a certain apparatus on the bus, includes a destination ID which represents an apparatus which should receive the packet inside the packet-header. When the destination ID represents a certain apparatus, an apparatus which is indicated by the identifier receives aforementioned asynchronous packet. When the destination ID represents broadcast, all apparatus on the same bus receive aforementioned asynchronous packet. Also,

asynchronous packet has, inside of packet-header, a source ID as an identifier which represents a sending apparatus that is sending the packet. The destination ID and the source ID have respectively been assigned 16 bit, and in 10 bit of them, a bus ID which identify a bus to which a device is connected is written in, and in 6 bit of them, a node ID which identify aforementioned device on the bus.

[0006] Additionally, IEC61883 specification (hereinafter described as "AV protocol") is considered in IEC(IEC: International Electronical Commission) as a specification for conducting a connection management of data transfer between devices on IEEE 1394 bus, and a transfer digital audio signal and digital image signal and the like with the use of IEEE 1394 specification. In AV protocol, image audio data is transferred disposed inside the isochronous packet. Additionally, the isochronous packet includes CIP header (CIP: Common Isochronous Packet). The CIP header includes information such as identification data which represents type of image audio data or a source ID as an identifier which represents sending apparatus of sending isochronous packet.

[0007] Figure 5 represents a format of isochronous packet which is in accordance with AV protocol. Isochronous packet consists of isochronous packet-header 900, header CRC 901, isochronous payload 902, and data CRC 903.

[0008] Isochronous packet-header 900 includes tag 907. Tag 907, when the value is 1, indicates that the isochronous packet is one which is in accordance with AV protocol. When the value of tag 907 is 1, in other words, it is one which is in accordance with AV protocol, CIP header 904 is included at the top of the isochronous payload 902.

[0009] Additionally, Channel field 911 in isochronous packet-header 900, is written channel code, and used as a

transfer on the bus.

[0010] Additionally, isochronous packet-header 900 includes Sy field 910. In an isochronous packet of AV protocol compliance, Sy field is used for storing the data protect information (use license information). Specifically, it includes 2 bit information which indicates representative value of use license information (it is called EMI; Encryption Mode Indicator) and data encryption mode and 1 bit information which is called as Odd/Even flag which indicate renewal timing of data encryption key. When the value of EMI which is stored in Sy field 910 indicates 「00」, it indicates data to be sent(actual data 905 described later) is a data that is free to copy. Additionally, when it is 「10」, the data shows that only one time copying is possible, and when it is 「11」, it indicates the data is copy inhibited.

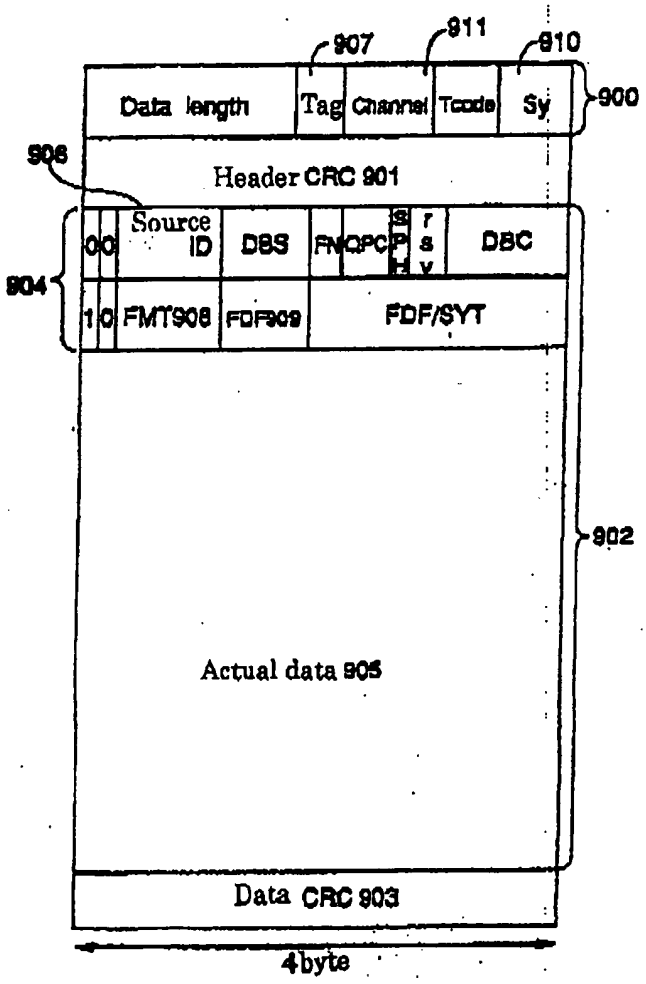
[0011] In the CIP header 904, a source ID 906 which is an identifier of source apparatus which is outputting aforementioned isochronous packet. This source ID 906 has 6 bit in length, and a node ID that identifies the apparatus of aforementioned source in one bus.

[0012] Additionally, the CIP header 904 includes FMT 908 that represents that what kind of data the actual data 905 in isochronous payload 902 or FDF 909.

[0013] Data as objects to be sent such as image and audio are included in actual data 905. This actual data 905 is encrypted data when above-mentioned EMI value is 「10」 or 「11」, while when it is 「00」 which means copy free, it is not encrypted. Additionally, actual use license information is included in the actual data 905,and generally it is called as SCMS, in case of CD, and it is called as such as CGMS in case of DV.

(2) Figure 5 is attached hereto.

[Fig.5]


907
911
910
Data length
Tag
Channel
Tcode
Sy
900
906
Header CRC 901
Source ID
DBS
FN
QPC
SP
rsv
DBC
904
1
0
FMT908
FDF909
FDF/SYT
902
Actual data 905
Data CRC 903
4byte